Third Party Acceptable Usage Policy

VicTrack Policy

Document information

Doc ref no: D/25/9115

Controlled doc no: VT-PO 215

Approved: 30 July 2025

Review: 30 July 2027

Version: 1.0

Distribution This document is to be shared with Third Party suppliers with access to VicTrack's ICT systems, networks or data.

Contents

Definitions

Term	Definition
Artificial Intelligence (AI)	The simulation of intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using the rules to reach approximate or definite conclusions), and self-correction.
Information (Assets)	Any hardware or software asset associated with information (or data), including its processing and storage, such as laptops, mobile phones, databases, documents, network devices, and removable devices like USBs and memory sticks.
ICT (systems)	Information and Communication Technology (ICT) systems refer to the integrated set of hardware, software, networks, applications and processes used for collecting, storing, processing, transmitting, and displaying information.
Intellectual Property	The term 'Intellectual Property' refers to the set of legal rights that protect the results of creative efforts including literary, artistic and scientific works, performances, broadcasts, inventions, scientific discoveries, trademarks and designs.
Must	The use of the word "must" within the Policy statements of this document implies that the Policy statement is mandatory to be implemented within VicTrack.
Should / Shall / Will	The use of the word "should" within the Policy statements of this document implies that the Policy statements denote a guideline or recommendation whenever non-compliance with the specification is permissible.
Public Locations	Any spaces that are accessible by the general public, including third-party locations that are not VicTrack managed or owned, where there is a higher risk of unauthorised access to VicTrack Information Assets. Examples include airports, cafés, restaurants, libraries, public transportation, hotel lobbies, and any other areas where controlled access is not possible.
Social Media	Any online platforms and technologies that facilitate the creation, sharing, and exchange of information, ideas, opinions, and other forms of expression through virtual communities and networks, such as Facebook or LinkedIn.
Suspicious or Untrusted Sources	Emails with/without attachments that could be phishing emails with the following characteristics: • Originate from senders where the email address is inconsistent in spelling or include unfamiliar email domains • Use language that creates a sense of urgency, fear or prompt immediate action • Contain unusual or unexpected requests for personal information or financial details • Use generic greetings instead of a person's name.

Term	Definition
Third Party	Refers to any external entity that interacts with VicTrack's ICT Systems, data, or services such as vendors, suppliers and service providers.
Users	Refers to any external individual or entity that has been granted access to VicTrack's Information and Communication Technology (ICT) systems, applications, and data including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

1. Purpose

The Third Party Acceptable Usage Policy (the "Policy") defines VicTrack's position regarding the appropriate use of Information Communication and Technology (ICT) systems and data by Third Parties. This Policy is in place to ensure that all use of VicTrack's ICT systems and data is consistent with the aims, values, and objectives of the organisation.

2. Scope

The scope and coverage of this Policy includes:

People	Organisational Locations	Technology
Third Party suppliers with access to VicTrack's ICT systems, networks, data or physical assets.	This Policy applies to Third Party suppliers with access to VicTrack ICT systems or networks regardless of work location.	All ICT systems or applications that store, process or transmit VicTrack's information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3. Responsibility Statement

All Third Party suppliers with access to VicTrack's ICT systems, networks or data ***must*** ensure that they have read and understood this Policy.

4. General Statements

1. All Users ***must*** familiarise themselves with this Policy prior to using VicTrack's ICT Systems and services.
2. All Users **must** be aware that all activities on VicTrack's ICT systems are electronically monitored and logged.
3. VicTrack reserves the right to access, monitor, and disclose the contents and activities of an individual User's account(s) and their activities when accessing VicTrack's ICT systems and resources.
4. VicTrack may monitor, access, record and/or make available, any data generated by ICT systems.

5. Email Usage (including Social Media usage)

1. Users ***must*** not use their provided VicTrack email address (if any) or other VicTrack related identities to register with Social Media websites or any other non-work related websites.
2. Users ***must*** use their VicTrack provided email (if any) only to fulfill VicTrack business and role-oriented tasks.
3. Email access will be terminated when the third-party terminates their association with VicTrack.
4. When using VicTrack provided email (if any), Users ***must not*** open, execute or store emails and/or attachments received from Suspicious or Untrusted Sources.

6. Device Security

1. Users ***must*** secure and protect their mobile phones from theft or compromise, as mobile phones will be used for multifactor authentication into VicTrack's ICT systems.
2. Users ***must*** ensure that any device used to access VicTrack ICT systems is regularly patched, updated with the required software and physically secured.
3. Users ***must*** ensure that their laptops and mobile devices are encrypted to protect sensitive data.
4. Users ***must*** log out or lock systems when not in use.

7. Configuration and Installation

1. Users ***must not*** install unauthorised software on any computers, laptops, network equipment, servers or other devices owned, managed or provided by VicTrack to access VicTrack ICT systems and data.
2. Users ***must not*** change configuration of ICT systems, or any other devices owned, provided or managed by VicTrack without following the relevant operational procedures and obtaining authorisation.
3. Users ***must not*** attempt to bypass, test, or tamper with the ICT security measures and services in place for VicTrack systems.
4. Users ***must not*** perform actions on a VicTrack device or within the VicTrack network that may put the network at risk.

8. Access Control

1. Users are responsible for all events that occur under their User accounts.
2. When accessing VicTrack's ICT systems, Users ***must*** use strong passwords accounting for the following requirements:
    a. ***Must*** be 16 characters long.
    b. ***Must*** include a mix of uppercase letters, lowercase letters, numbers, and special characters (e.g., @, #, $, %).
        i. At least 1 uppercase letter
        ii. At least 1 lowercase letter
        iii. At least 1 number

iv. At least 1 special character

3. Users are responsible for keeping their accounts and passwords confidential.
4. Users ***must not*** share their login credentials with any other person under any circumstances.
5. Users ***must*** access VicTrack ICT systems, applications, and data exclusively through CyberArk Remote Access or Microsoft Teams requiring the use of Multifactor Authentication (MFA).
6. Users ***must*** report an account or password suspected of being compromised, or an attempt made to compromise an account or password to the VicTrack Network Management Centre (NMC).
7. Users ***must not*** store passwords used to access VicTrack's ICT systems or information assets in unsecured formats such as Microsoft Word, Excel, or OneNote.
8. Users ***must not*** access VicTrack ICT systems while connected to untrusted networks such as any public Wi-Fi.

9. Data Security

1. All documents, data, and applications created for VicTrack, or while using or accessing any VicTrack ICT Systems, remain the intellectual property of VicTrack and ***must*** be used solely for VicTrack work-related purposes.
2. The unauthorised copying, distribution or use of copyrighted material is prohibited and in breach of the *Copyright Act 1968 (Link)* (this includes the playing of pirated music or videos on VicTrack ICT Systems).
3. Data ***must*** be transferred only via approved secure transfer mechanisms, for example VicTrack sanctioned Microsoft OneDrive, and Microsoft Teams.
4. All Users ***must*** protect VicTrack Information Assets in Public Locations by not leaving them unattended and ensuring they are not visible to unauthorised personnel.
5. Users ***must*** not copy or transfer VicTrack data onto portable devices (for example, USB), to any cloud-based storage (such as Google Drive, Dropbox etc.) or to any Artificial Intelligence (AI) system or application without prior authorisation from VicTrack.

10. Incident Reporting

1. Users ***must*** be aware of cyber incident notification requirements and report security incidents promptly. These requirements are stated in VicTrack's Third Party Information Security Requirements.
2. Third Parties ***must*** notify VicTrack within 12 hours of any actual or suspected cyber incidents that may have a Significant Impact. These are cyber events or incidents that may directly impact VicTrack and hinder its ability to deliver services including (without limitation) any impact to transport or telecommunications infrastructure which is integral to Victoria's transport system.
3. Third Parties ***must*** notify VicTrack of any actual or suspected cyber incidents that are not classed as Significant Impacts within 72 hours.
4. Users ***must*** assist VicTrack in cyber incident response activities if VicTrack issued credentials are involved in any incident, or if there is any suspicion of a third party's ICT Systems or networks being involved in the incident.

11. Physical Security

1. Users ***must*** adhere to VicTrack's physical security requirements when visiting VicTrack facilities, including signing in upon arrival and receiving a visitor badge.
2. Users ***must*** only access physical locations at VicTrack's facilities that are necessary for the services they are engaged to provide to VicTrack.

12. Enforcement and Compliance

Compliance with this Policy and all related documents is mandatory for Third party suppliers with access to VicTrack's ICT systems, networks, data or physical assets.

VicTrack may change, alter, modify, or discontinue any of its policies, including this Policy, in accordance with other applicable VicTrack policy, processes and procedures.

13. Document history

Version	Amendment description	Author	Date
Version 1.0	First version	Manager Enterprise Architecture & Security	25 July 2025

14. Review period

This policy will be reviewed at least every two (2) years by the Executive, or amended as appropriate.

The content of this document is uncontrolled when printed. The current version of this document is available on The Loop.